MOTION PICTURE ASSOCIATION OF AMERICA

MPAA Views on Revocation Processing in the Broadcast Flag Application

Brad Hunt
MPAA Chief Technology Officer
July 21, 2004

In its Report and Order on Digital Broadcast Content Protection, the FCC described seven "functional criteria" that they would use as "key evaluative factors" in their certification process of digital output protection technologies and secure recording methods for use in the Broadcast Flag application. These functional criteria included "level of security, scope of redistribution, means of authentication, upgradeability, renewability, interoperability, and ability to revoke compromised devices." This last criteria concerning revocation is an important aspect of a content protection technology and can be described as the ability of a content protection technology to provide a means to revoke the digital key or certificate associated with a device's ability to authenticate and gain access to content protected using the licensed technology.

The continuing effectiveness of a content protection technology greatly relies on support for device key revocation. It must be accepted that, given enough resources and time, hackers will be able to gain access to a content protection technology's secret device key contained within a single compliant device. This single device key can be used to produce an unlimited number of non-compliant "clone" devices that ignore all copy protection requirements. When the licensor of the content protection technology becomes aware of non-compliant clone devices in the marketplace, they can determine the clone devices' secret device key being used and then issue a System Renewability Message that revokes this device key, along with any other illegally obtained individual device keys. Although the term "system renewability" typically refers to the capability of a far more comprehensive renewal of the security components of a content protection system, in this case, content protection technology developers refer to their device key revocation list as a "System Renewability Message" (SRM).

The developers of content protection technologies provide clear specifications for their System Renewability Message files. To effectuate revocation, the content protection licensor generates a new SRM file and then provides it to content providers, MVPDs, and broadcasters, who in turn deliver these SRMs with the content. For example, in the case of the DVD Content Scrambling System, which has approved HDCP-protected outputs, the HDCP SRM is delivered on the DVD disc as a HDCP.srm file. This SRM file is read from the DVD during playback and then conveyed to the HDCP function for SRM revocation processing. If a cloned HDCP device is connected to a DVD player playing a CSS-encrypted DVD, the cloned device will be detected during HDCP revocation processing and the DVD CSS player will stop the flow of digital content to the HDCP digital output. The DVD player will continue to operate properly with its other video outputs enabled. It should be understood that content protection device key revocation does not totally disable an entire device. It only disables the particular digital protected output or the secure recording method of the device having the cloned or illegally acquired content protection device key.

In order to have an efficient means for carrying and conveying downstream a variety of SRMs in the digital content, a number of CE and IT companies have been working on defining a common specification for the carriage of SRM files in MPEG-2 Transport Streams. Since these SRMs must be carried in both the ATSC Transport Stream as transmitted by the broadcaster and in a subsequent derivative MPEG-2 Transport Stream output from the ATSC receiver, one possible approach would be to define a Private Data Type within the Program Map Table (PMT) for associated data related to content protection SRMs. The PMT is carried in both the ATSC Transport Stream and the MPEG-2 Transport Stream. With the stored SRM information defined in the PMT, this information could be easily conveyed downstream in the MPEG-2 Transport Stream supplied to authorized digital protected outputs and secure recording methods.

The MPEG-2 Systems standard already defines the structure for carriage of private data using the Program Map Table. Once a standard is adopted by the ATSC, the SRM could be inserted as private data and identified as such in the PMT prior to transmission. Until such time that an ATSC standard is developed for carrying SRMs in other compressed digital video formats, all compressed digital output and digital recording of Marked and Unscreened Content has to be done in the MPEG-2 Transport Stream format. This is not a new requirement since this must be done today in order to support interoperability among digital television displays and digital recording devices.

Effective revocation processing relies on the latest, up-to-date SRMs to be delivered in the most recent program broadcasts in order to address new “clone” attacks that surface and to correct the effect of any earlier mistaken or cured device revocations. In addition, SRMs must also be conveyed to downstream devices because some content protection technologies, such as the High-bandwidth Digital Content Protection (HDCP), do not store their revocation lists. These content protection technologies must rely on real-time processing of SRMs contained in the content to achieve effective device revocation.

An effective revocation infrastructure is a critical component in achieving the Commission’s goal of facilitating the digital transition and preserving the free-to-air broadcasting system from migration of high value programming to more secure delivery systems. In order for the Broadcast Flag to support effective content protection device key revocation, the following steps should promptly be taken.

1) The FCC should request that the ATSC T3 Technology Group launch a standards activity to define a Private Data Type within the Program Map Table (PMT) for associated data related to content protection System Renewability Messages. This would allow the standardized insertion and carriage of the various SRMs in MPEG-2 Transport Streams and in ATSC Transport Streams. This standard would define how broadcasters insert SRMs into their ATSC broadcast streams and how Covered Demodulator Products identify and parse these SRM files in the transport stream in order to pass them to the content protection technologies implemented in the Covered Demodulator Product.

2) The FCC should clarify in its interim content protection technology certification report or no later than in connection with its pending Digital Broadcast Content Protection FNPRM that when an authorized digital output protection technology or an authorized recording method is implemented in a Covered Demodulator Product, then the Covered Demodulator Product must preserve and convey the embedded SRMs in Marked and Unscreened Content to all those content protection technologies implemented in the Covered Demodulator Product. In addition, the FCC should also clarify as part of its pending Digital Broadcast Content Protection FNPRM that the Covered Demodulator Product must also preserve the embedded SRMs in Marked and Unscreened Content when passing this content through any authorized digital output, including those using a Robust Method, or when making any authorized recording, including a non-transitory bound recording of this content.

3) The FCC interim and later approval of any content protection technology certification should include confirmation that the licensor of the technology has: (i) defined a process for device key revocation; (ii) documented the specifications for their SRM digital file; (iii) specified its private data identifier in the PMT (after ATSC standardization is completed); and (iv) obligated its licensees to preserve and convey downstream all SRMs in Marked and Unscreened Content related to any content protection technology authorized under its license. This latter requirement is critical for ensuring that SRMs for all approved content protection technologies that rely on real-time revocation processing are delivered to and processed by Downstream Covered Products.

4) In the case of FCC interim and later approval of a digital output protection technology, the FCC order should include an associated obligation that the digital output protection technology upon receipt of content containing SRMs must: (i) process any of its own SRMs to prevent revoked devices from gaining access to Unscreened and Marked Content and (ii) preserve and convey downstream all SRMs in its MPEG-2 transport stream in Marked and Unscreened Content for all digital outputs, all approved digital output protection technologies, all authorized, non-transitory bound recording methods, and all authorized secure recording technologies that are approved under its license.

For example, the 5C Digital Transmission Content Protection (DTCP) technology authorizes the use of 4C Content Protection for Recordable Media (CPRM) technology for secure recording. And both the 5C DTCP and 4C CPRM technologies authorize the use of High-bandwidth Digital Content Protection (HDCP) technology for protected digital outputs. Therefore, DTCP must preserve and convey downstream any received HDCP SRMs in the DTCP protected MPEG-2 transport stream outputs and in any subsequent CPRM-protected recordings. This is graphically described in the attached informative example drawing showing a Broadcast Flag compliant DTV Receiver connected using an IEEE 1394 interface to a DVD Recorder capable of making 4C CPRM-protected DVD recordings that can played out over a HDCP-protected DVI output. The HDCP SRM is preserved in the DTCP-protected MPEG-2 transport stream output from the DTV Receiver to the DVD recorder and is subsequently preserved in the CPRM-protected DVD recording. When the CPRM recording is played, the HDCP SRM is sent to the HDCP function to enable revocation processing.

5) In the case of FCC interim or later approval of an authorized recording method that delivers its revocation list information on blank recordable media, the FCC order should include an associated obligation that the authorized recording method upon receipt of SRMs must: (i) preserve all received SRMs in its protected MPEG-2 recordings and (ii) subsequently convey downstream all SRMs in its MPEG-2 transport stream recordings of Marked and Unscreened Content for all digital outputs, all approved digital output protection technologies, all authorized, non-transitory bound recording methods, and all authorized secure recording technologies that are approved under its license.

For example, the 4C CPRM technology carries its revocation list information on blank CPRM-enabled media. But the CPRM technology authorizes HDCP outputs on the playback of CPRM encrypted recordings. Therefore, when CPRM preserves HDCP SRMs in its protected MPEG-2 DVD recordings, these HDCP SRMs can be conveyed to the HDCP function during playback of the CPRM-protected DVD in order to facilitate real-time HDCP revocation processing.

The attached drawing goes on to describe how SRM preservation and conveyance is handled during serial digital copying of Marked Content. As illustrated in this informative example, when a DVD+RW recorder with Vidi content protection technology attempts to make a digital copy from the playback of the CPRM-protected recording using a DTCP-protected digital connection, the HDCP SRM must be conveyed and then preserved in the MPEG-2 transport stream sent to and in the MPEG-2 recording made by the Vidi recorder. In this way, when the Vidi-protected DVD recording is played, the HDCP SRM can be conveyed to the HDCP function to enable revocation processing.

6) In the case of FCC interim or later approval of an authorized recording method that does not deliver its revocation list information on blank recordable media, the FCC order should include an associated obligation that the authorized recording method upon receipt of SRMs must: (i) process any of its own SRMs to prevent revoked devices from gaining access to Unscreened and Marked Content; (ii) preserve all received SRMs in its protected MPEG-2 recordings; and (iii) subsequently convey downstream all SRMs in its MPEG-2 transport stream recordings of Marked and Unscreened Content for all digital outputs, all approved digital output protection technologies, all authorized, non-transitory

bound recording methods, and all authorized secure recording technologies that are approved under its license.

There have been questions raised as to what steps can be taken in implementing device key revocation at this time given that ATSC standards for carriage and delivery of SRMs do not yet exist. Since revocation processing is an important feature in determining the effectiveness of a content protection technology, the regulatory and license obligations for carriage, conveyance, and processing of SRMs should be put in place now, with appropriate grace periods defined, where necessary, from the time when the ATSC standards work is completed.

To summarize, the FCC Interim Certification report or the Digital Broadcast Content Protection FNPRM should clarify the requirement that Covered Demodulator Products must preserve and convey downstream all valid received SRMs, as defined above. The associated obligations relating to the digital output protection technologies and authorized recording methods being certified should also be stated at the time of interim approval with an 18 month implementation grace period granted from the time the ATSC SRM carriage standards are published. Simultaneously, the FCC should explicitly request the ATSC to begin the standards work. These steps should be taken now in order for the Commission to achieve the objectives of the regulation.